uPlanner

Política de Seguridad de la Información

/uplanner /company/u-planner /u-planner /uplannerEducation

1 Objetivo

Establecer las políticas, prácticas y lineamientos internos de Seguridad de la Información para uPlanner con el fin de asegurar la protección de los activos de información en todas sus formas y medios contra su modificación accidental o deliberada, utilización no autorizada, divulgación o interrupción, de modo de garantizar su confidencialidad, integridad y disponibilidad.

uPlanner establece que ante cualquier presentación legal que se requiera y esté relacionado con los sistemas informáticos o los usuarios internos, se observarán las leyes vigentes mediante el asesoramiento legal respectivo, para asegurar los requisitos regulatorios que apliquen.

2 Alcance

Este documento se aplica en todas las fases del ciclo de vida de la información (generación, distribución, almacenamiento, procesamiento, transporte, consulta y destrucción) y de los sistemas que la procesan (análisis, diseño, desarrollo, implementación, explotación y mantenimiento).

Aplica a todos los sectores de uPlanner, es decir, a todo el personal, tanto interno como externo; así como a las personas que directa o indirectamente prestan sus servicios profesionales dentro de la misma, y a toda la información obtenida, creada, procesada, almacenada o intercambiada dentro y desde la Compañía.

3 Vigencia

Su vigencia será a partir de **01/04/2022**.

4 Responsabilidades

- El **CEO** es el director con responsabilidad general de la seguridad de la información de toda la organización.
- El **COO** es el director con responsabilidad general sobre la estrategia operativa de seguridad de TI.
- El **Senior Cloud Systems Administrator (SCSA)** tiene la responsabilidad operacional diaria de hacer que estas políticas se implementen.
- **Team Leader Platform (TLP)** es el oficial de protección de datos que va a asesorar en leyes de protección de datos y las mejores prácticas.

5 Autoridad de emisión, revisión y publicación

Esta Política ha sido desarrollada por el **Senior Cloud Systems Administrator (SCSA)** y aprobada por la Alta Dirección de uPlanner.

Se revisará al menos anualmente, y será modificada según las necesidades y evolución del negocio.

Este documento y los que se generen de él, deberán ser publicados y comunicados a toda la compañía y a todos los niveles de la organización.

6 Reglas de aplicación

6.1 Designación de un oficial de protección de datos

El oficial de protección de datos es designado por sus cualidades profesionales y conocimiento específico en leyes y prácticas de protección de datos. **uPlanner** designa este rol al profesional: **Team Leader Platform.**

La empresa debe asegurar y proveer al área de protección de datos con todos los recursos apropiados para realizar sus labores y mantener su conocimiento a un nivel de experto en la materia.

El oficial de protección de datos reporta directamente al nivel más alto de la gerencia y no tiene otras responsabilidades que resulten en un conflicto de intereses.

6.2 Gestión con instituciones de seguridad de la información

La gestión con instituciones de seguridad de la información tiene como objetivo mantener un contacto con organizaciones especializadas que puedan proporcionar apoyo para la implementación y mantenimiento del SGSI.

Considerando los requisitos de las partes interesadas y las regulaciones aplicables, uPlanner mantiene contacto con las siguientes organizaciones para la comunicación y reporte de los incidentes de seguridad:

Organizaciones	Contacto
Brigada Investigadora del Ciber Crimen de Policía de Investigaciones	Teléfono: 2 2708 0658 Correo electrónico: cibercrimen@investigaciones.cl
Brigada Investigadora Delitos Contra la Propiedad Intelectual	Teléfono: 2 2708 2366

Organizaciones	Contacto
Carabineros de Chile	Teléfono: 133
PDI	Teléfono: 134

Para asegurar la concientización y el conocimiento de los colaboradores, la empresa también mantiene contacto con grupos de interés especial que les permite capacitarse y estar actualizados sobre las mejores prácticas, nuevas amenazas, alertas y/o vulnerabilidades de seguridad.

Empresa | Institución	Medio de contacto
Hackmetrix	Blog, Hacknews (notificaciones sobre vulnerabilidades), Hackmeets (foros sobre temas de seguridad de la información).
Microsoft Tech News	Boletín mensual enviado por correo electrónico por parte de Microsoft, con información reciente relacionado a avances tecnológicos, noticias de productos y eventos.
uPlanner Seguridad de la Información	Equipo de Microsoft Teams para el envío de notificaciones sobre vulnerabilidades, cursos y temas de seguridad de la información a todos los usuarios uPlanner.

6.3 Gestión de Activos y Clasificación de la Información

La Gestión de Activos y Clasificación de la Información tiene como objetivo garantizar que los activos, constituidos por información, y los recursos que le dan soporte, sean identificados, inventariados y clasificados en función de los requerimientos del negocio.

El **CFO** debe establecer los procesos y procedimientos necesarios para una adecuada gestión de activos de acuerdo con las necesidades del negocio, los cuales deberán asegurar:

- La identificación y el mantenimiento del inventario de activos de Información.
- Establecer los mecanismos para la designación de Propietarios de Activos de Información.
- Establecer los criterios de clasificación de la información en función de las dimensiones de confidencialidad, integridad y disponibilidad, de acuerdo con el nivel de criticidad que la información tenga para el negocio.
- Establecer los procedimientos necesarios para la clasificación de la información y todos los activos de información que le dan soporte.
- Establecer los niveles mínimos de tratamiento de seguridad que deberá dar a la información de acuerdo con el nivel de clasificación de confidencialidad asignada, en términos de su ciclo de vida, generación, transmisión, utilización, guarda y destrucción.
- Los Propietarios de los Activos de Información deberán identificar, categorizar, modificar y dar de baja los activos de información en el inventario, como así también, determinar la clasificación de la información bajo su responsabilidad, en función de los criterios definidos por la Gerencia de Seguridad Informática.

Sólo se clasifica información que sea estrictamente necesaria para el funcionamiento de la empresa, y lo que no es estrictamente necesario quedará como no clasificado. También se limitan los accesos a los datos sólo para aquellos que lo requieran en el desempeño de sus tareas. La información se divide en categorías, para asegurar que está protegida de forma adecuada y que se están asignando los recursos de seguridad de forma pertinente.

- **No clasificado**: Es información que se puede hacer pública, sin que implique consecuencias negativas para la empresa, como es la información que es de conocimiento público.
- **Confidencial de los empleados:** Esto incluye información como registros médicos, salarios, entre otros.
- **Confidencial de la compañía:** Como contratos, códigos fuente, contraseñas para sistemas críticos de TI, contratos de clientes, cuentas, etcétera.

- **Confidencial del cliente:** Esto incluye información de identificación como nombre, dirección, claves de acceso al sistema de clientes, planes de negocio, información de nuevos productos, información sensible del mercado, etc.

Hemos categorizado la información que tenemos de la siguiente forma:

Tipo de Información	Sistemas involucrados	Nivel de clasificación	Propietario de la información
Registros de los clientes	Hubspot- Wordpress – Google Analytics - Teams	Confidencial de compañía	uPlanner
Registro de los empleados	BUK	Confidencial de la compañía	CPO - Chief People Officer y Administrative Officer
Registros de información financiera	Docs – Odoo	Confidencial de la compañía	CFO
Licencias médicas	Medipass	Confidencial de la compañía	Administrative Officer
Registro de vacaciones	BUK	Confidencial de la compañía	Administrative Officer
Registro de contratos clientes	DocuSign - Webdox	Confidencial de la compañía	CFO - CCO
Registro de contratos colaboradores	BUK	Confidencial de la compañía	CFO
Bases de datos	Azure	Confidencial de la compañía	uPlanner
Información Legal	Docs - OneDrive	Confidencial de la compañía	CFO

Tipo de Información	Sistemas involucrados	Nivel de clasificación	Propietario de la información
Estrategias de la compañía	Docs - Teams	Confidencial de la compañía	CEO
Documentación productos (Descriptivos, fichas técnicas)	Docs - Teams	No clasificado	COO
Casos de éxito	Teams - YouTube	No clasificado	Administrative Officer
Comunicación y operaciones	Office365, VPN, Jira Cloud, Bamboo	Confidencial de la compañía	Platform Team
Gestión del código fuente	Bitbucket	Confidencial de la compañía	Platform Team

Información más detallada se encuentra en otros repositorios y sistemas de información, además del inventario de activos de la organización.

6.4 Gestión de Riesgos

Este proceso tiene como objetivo ayudar a identificar y medir posibles eventos de pérdida (operativa y tecnológica) futuros y a establecer y priorizar planes de tratamiento sobre los riesgos que desafían sus objetivos estratégicos y prácticas operativas cotidianas de la empresa.

La gestión de riesgo busca además ayudar al **SCSA** a identificar y medir amenazas y vulnerabilidades que pongan en riesgo la confidencialidad, integridad y disponibilidad de la información de la compañía, en especial aquella más crítica para el desarrollo confiable e ininterrumpido de sus actividades, como así también, establecer y priorizar los planes de tratamiento para reducir riesgos.

El responsable deberá establecer un proceso formal que permita a la Alta Gerencia:

- Identificar los riesgos estratégicos que pueden afectar negativamente al logro de los objetivos estratégicos de la compañía.
- Definir y aprobar el alcance del proceso de gestión de riesgos y las modificaciones eventuales al mismo.
- Definir el umbral de tolerancia y aceptación de riesgos de la organización.
- Aprobar el nivel de riesgo residual de la organización.
- Identificar activos críticos, amenazas y vulnerabilidades.
- Establecer los criterios de evaluación, tratamiento y medición de riesgos.
- Definir la planificación de los análisis de riesgos.

El análisis y evaluación de riesgos se realizará, como mínimo, **anualmente** o cuando ocurran cambios significativos en el entorno, lo que suceda primero.

6.5 Gestión de Accesos y Perfiles

La Gestión de Accesos y Perfiles tiene como objetivo establecer los lineamientos para un adecuado control de todos los usuarios y perfiles utilizados por el personal de la compañía o terceros que accedan a los activos informáticos.

Internamente, en la medida de lo posible, operamos bajo la política de la "necesidad de compartir" y no la "necesidad de saber" esto es con respecto a la información confidencial de la empresa. Esto significa que nuestra parcialidad e intención es compartir la información para ayudar a la gente a realizar su trabajo y no para aumentar las barreras de acceso a la información innecesarias.

En cuanto a la información del cliente, operamos bajo el principio de "El derecho de acceso" de GDPR. Esto hace referencia al derecho de los dueños de la información a confirmar el procesamiento de sus datos, dónde se procesa y con qué propósito. De forma adicional, tenemos que proporcionar, si es que nos solicitan, una copia de sus datos personales, sin cobrar por ello y en un formato electrónico.

Se permite que los interesados transmitan sus propios datos a otros controladores.

Adicionalmente, los privilegios de administrador de los sistemas de la empresa son restringidos a individuos específicos y autorizados, para las siguientes funciones que le permiten desarrollar su trabajo de forma correcta. Esta información se encuentra en la **matriz de control de accesos de la compañía**.

Como medidas de precaución para la preservación de la información se adoptan los siguientes lineamientos:

- Todo usuario de sistemas o plataformas tecnológicas está asociado a una persona física de manera unívoca y en los casos que se requiera la utilización de usuarios genéricos, estos tengan un responsable asociado.
- Se establece una gestión de las altas y asignación de credenciales de usuarios considerando la identificación de estos y las autorizaciones necesarias para su gestión.
- Ante un cambio de funciones se eliminan los accesos relacionados con la función anterior y se asignan los accesos necesarios para la nueva función.
- Toda desvinculación de personal implica el retiro de los accesos otorgados y/o la eliminación o inhabilitación de los ID de usuarios asociados a la persona.
- Se asegura la adecuada segregación de funciones evitando la asignación de permisos incompatibles con las funciones de los usuarios.
- La generación/acceso a los usuarios de privilegios especiales en los sistemas y plataformas se encuentre limitado a personal debidamente identificado y bajo una adecuada justificación de necesidad, como así también que su utilización sea monitoreada y controlada.
- Existe una adecuada custodia de las credenciales de usuarios de privilegios especiales y usuarios genéricos que asegure la identificación del personal que las utilice y el registro de la justificación para su utilización.
- En vistas de mantener la asignación de manera correcta, se ejecutan revisiones periódicas validando la **matriz de control de accesos y permisos** en las aplicaciones críticas de la empresa (Office365, VPN, Jira, Bamboo, Bitbucket)

- En vistas de mantener la asignación de manera correcta, cada vez que un profesional deja la compañía o uno nuevo ingresa, se realiza la revisión de derechos de accesos que está a cargo del System Administrator y se ejecuta de la siguiente manera:

  1.- Revisión de accesos y permisos de Office 365

  2.- Revisión de accesos mediante VPN

  3.- Revisión de acceso a Bitbucket

  4.- Revisión de accesos a Jira Cloud

  5.- Revisión de accesos a Bamboo

6.6 Gestión de Seguridad de Entornos, Plataformas y Aplicaciones

La Gestión de Seguridad de Entornos, Plataformas y Aplicaciones tiene como objetivo establecer los lineamientos para la definición, implementación y control de una adecuada seguridad en todos los entornos y plataformas que soportan los servicios de negocio.

Para proteger los datos, sistemas, usuarios y clientes se usan los siguientes sistemas:

Antimalware para computadoras portátiles y de escritorio - **Windows Defender**.

- Email spam, malware y filtrado de contenido alojados en la nube - **Políticas de seguridad de Office 365**.
- Archivos y continuidad de correos electrónicos - **Office 365**.
- Análisis de vulnerabilidades y malware del sitio web – **Nessus y Fortify**.
- Detección y prevención de intrusión - **Azure Defender y Azure Sentinel**.
- Firewall de escritorio - **Windows Firewall**.
- Firewall perimetral - **Azure Firewall**.
- Web Application Firewall - **Azure WAF**.

- Administración de costos en la nube - **Cloud Health**.

Adicionalmente, se desarrollan estándares de hardening basado en el top 10 de OWASP que deberán contemplar como mínimo las definiciones necesarias para las siguientes categorías de entornos, plataformas, sistemas o aplicativos:

- Sistemas operativos.
- Redes y dispositivos de Red.
- Sistemas de almacenamiento.
- Sistemas de virtualización.
- Bases de datos.
- Aplicaciones en general.
- Aplicaciones web.
- Soluciones de seguridad.

Todo cambio de arquitectura, infraestructura o definiciones de seguridad deben ser acordados con el **Platform Team** a fin de no generar problemas de seguridad. Este paso consiste en poder entregar todo el contexto al equipo de plataformas para poder abordar la solución bajo todas las políticas de seguridad implementadas.

Es por esto, que se deben considerar los siguientes lineamientos:

Gestión de la seguridad de redes

- Las redes deben gestionarse y controlarse adecuadamente para proteger la información en los sistemas y aplicaciones de uPlanner.
- Restringir las conexiones entre redes no confiables y cualquier componente del sistema en los entornos críticos.
- Se prohíbe el acceso público directo entre Internet y todo componente del sistema en los entornos críticos.

- Las políticas y los procedimientos operativos para administrar los equipos de red deben estar documentados, implementados y ser de conocimiento para todas las partes afectadas.

Intercambio de información con partes externas

- uPlanner debe implementar políticas, procedimientos y controles formales para proteger el intercambio de información por medio del uso de cualquier tipo de recurso de comunicación, en coherencia con las políticas de clasificación de los activos de Información.

6.7 Gestión de la seguridad de los servicios de aplicaciones

- Se deben contemplar controles para que las transacciones en la página de la organización se ejecuten de manera segura. Algunos que se contemplan, pero que no son limitativos, son: uso de certificados, uso de firma electrónica, uso de autenticación de usuarios, encriptación de protocolos de comunicación entre las partes involucradas, etc.

6.8 Gestión de Vulnerabilidades

La Gestión de Vulnerabilidades tiene como objetivo detectar las exposiciones de posibles vulnerabilidades que puedan encontrar y aprovechar personas malintencionadas. Una correcta ejecución y detección temprana ayuda a reducir el riesgo de exposición.

Dado esto, se dictamina lo siguiente:

- Se realizará Ethical Hacking cada 12 meses.
- Se debe establecer un proceso formal de gestión de vulnerabilidades que contemple:
    - La realización periódica de escaneos de vulnerabilidades y pruebas de intrusión.
    - La verificación periódica de la publicación de vulnerabilidades por parte de los fabricantes de tecnología.

- Se definan plazos para reaccionar ante las notificaciones de vulnerabilidades técnicas potencialmente relevantes de resolución que contemple, como máximo, **10 meses**. Esto está sujeto a implementar un parche inicial que subsane las principales vulnerabilidades dentro del primer mes, para luego implementar la solución definitiva dentro del plazo máximo.
- El análisis de aplicabilidad de las vulnerabilidades detectadas o identificadas y la definición de su remediación.
- Generación de un plan de remediación con plazos establecidos y su seguimiento.

6.9 Gestión de Incidentes (de seguridad)

La Gestión de Incidentes tiene como objetivo establecer lineamientos para un adecuado registro, análisis y tratamiento de los incidentes de seguridad que puedan afectar a la compañía.

Por tal, se considera lo siguiente:

- Se debe registrar, analizar y definir mitigantes, si correspondiera, para todo incidente de seguridad reportado o detectado.
- Todo el personal debe informar al área de plataformas todo evento que pueda considerarse un incidente de seguridad.
- El **área de plataformas** debe establecer un proceso formal de gestión de incidentes de seguridad que permita un adecuado registro de estos, su priorización, análisis y seguimiento hasta su cierre.
- Ante un incidente detectado, existe un equipo experto en remediar los mismos, así como otras vulnerabilidades detectadas.
- También, se debe analizar los incidentes de seguridad ocurridos, el impacto ocasionado, su frecuencia y forma de resolución aplicada, con el objeto de tener estadísticas de comportamiento de respuesta ante incidentes, aprender de lo ocurrido y establecer mejoras en las acciones de control y las políticas cuando sea necesario.

- Tener en cuenta los incidentes ocurridos en los futuros planes de concientización y capacitación.

6.10 Gestión del Ciclo de Vida, Puesta en Producción y Entornos

La Gestión del Ciclo de Vida, puesta en producción y entornos tiene como objetivo establecer los lineamientos para un adecuado control de los cambios, la puesta en producción y la segregación de ambientes.

Se debe establecer, documentar e implementar un proceso formal para el control de los cambios en producción y el pasaje de desarrollos al ambiente productivo, este proceso deberá contemplar:

- Autorizar la instalación de todo nuevo producto o modificaciones a sistemas aplicativos.
- Verificar que se hayan cumplido con todos los puntos de control existentes para los desarrollos/mantenimientos/adquisiciones de sistemas aplicativos de acuerdo con las metodologías de desarrollo, mantenimiento y adquisición de la compañía.
- Minimizar la posibilidad de modificaciones a los sistemas de aplicación durante los procesos de control y una vez aprobados e instalados en producción.
- Llevar un registro de todas las instalaciones efectuadas en el ambiente de producción. En la misma se debe indicar, mínimamente, fecha, hora, ambiente de procesamiento, identificación, activo de información y responsable interviniente.
- La seguridad correspondiente a todo nuevo desarrollo/modificación se debe adecuar a lo establecido por las normas y estándares de seguridad definidos.
- Establecer un procedimiento de emergencia para dejar sin efecto en forma rápida los cambios efectuados y poder recuperar las versiones autorizadas anteriormente en el caso de generarse problemas no solucionables durante la instalación y período de control que afecten a la continuidad operativa.

- Las aplicaciones existentes en el ambiente de producción deben estar debidamente documentadas cubriendo el detalle de las últimas funcionalidades y su uso en el sitio doc.uplanner.com. Internamente en el proceso de gestión del release deben estar identificados todos los cambios y versiones de cada microservicio en bitbucket y bamboo.
- Los ambientes están segregados en entornos de desarrollo, testing y producción.
- No utilizar datos productivos de clientes para realizar las pruebas.

6.11 Gestión de Capital Humano

El **CPO – Chief People Officer** debe establecer todos los lineamientos y procesos necesarios para asegurar la gestión de la seguridad relacionada con la incorporación, permanencia y desvinculación del personal que realizará tareas como colaborador de la Compañía, debiendo tener en cuenta los siguientes requerimientos:

- Formalización de los roles y responsabilidades de cada puesto dentro de la compañía, mediante los cuales realizar una evaluación de idoneidad y aplicabilidad del personal a incorporar.
- Aceptación por parte del colaborador de los términos y condiciones de contratación y las políticas y Normas de Seguridad de la compañía que debe cumplir.
- Formalización de un compromiso de confidencialidad y lealtad de acuerdo con lo que se establece en este documento.
- Formalización de un proceso para la desvinculación de colaborador considerando que permita un adecuado retiro y/o devolución de todos los activos provistos por la compañía y el retiro de todos los privilegios de acceso a los sistemas informáticos o físicos.
- Inducción a los colaboradores (internos y/o externos) sobre temas específicos de Seguridad de la Información. En caso de no brindar inducción o capacitación directa al colaborador externo, se debe exigir lo mismo a la empresa tercerizadora de personal.

- Formalización del código de conducta de la organización donde se detallen los valores, pautas y conductas que los colaboradores (internos y/o externos) deben respetar.
- Todos los empleados de la organización deben al menos una vez al año hacer una declaración de que leyeron y entendieron las políticas de Seguridad de la Información.

- Realizar un plan anual de capacitación y concientización sobre Seguridad de la información para colaboradores (internos y/o externos).

Se realiza entrenamiento a las nuevas incorporaciones y se entrega apoyo al personal existente para implementar esta política. Esto incluye:

- Una introducción inicial a la seguridad TI, cobertura de riesgos, medidas básicas de seguridad, políticas de la compañía y dónde encontrar ayuda.
- Entrenar como se usan los sistemas de la empresa y los softwares de seguridad de forma apropiada.
- Si se requiere, una revisión de salud de seguridad en sus computadores, tabletas o teléfonos, previo al ingreso del empleado.

Sanciones:

Puede ocurrir el caso en que personal interno, externo o proveedor incurra en alguna desviación o incumplimiento de esta política, lo cual puede ser motivo de sanciones administrativas e incluso legales que deben quedar explícitas en los contratos celebrados.

Teletrabajo:

Consistencia con la clasificación de la información.

Al trabajar de forma remota o en movimiento, los colaboradores y terceros externos, se asegurarán de que la Información se maneje de acuerdo con las Políticas de Seguridad de la información dispuesta por uPlanner, para cada una de las tareas y responsabilidades realizadas en el marco de la relación laboral.

Precauciones en entorno no seguro

El trabajador remoto tiene la responsabilidad de proteger los activos de información proporcionados por **uPlanner** ante cualquier tipo de acceso no autorizado a la información clasificada que surja de un entorno sin restricciones, por ende, no seguro. Específicamente:

- Debe tomar medidas para garantizar que el entorno ofrezca un nivel adecuado de privacidad (es decir, que terceros no puedan ver documentos o pantallas en los que se está trabajando o escuchar conversaciones privadas) antes de trabajar en cualquier información clasificada de **uPlanner**.
- El trabajador remoto nunca debe dejar documentos o equipos que contengan información clasificada o confidencial sin supervisión fuera de las instalaciones de **uPlanner**, a menos que estén debidamente protegidos contra robos o divulgación.
- El trabajador remoto debe asegurarse de que toda la Información de **uPlanner**, cuando corresponda, se elimine de acuerdo con la política de eliminación segura de activos de la Información.
- En el caso que necesite utilizar equipos de terceros, lo hará sólo en casos de emergencia, utilizando una sesión o ventana en modalidad “incógnito” para asegurar que no se puedan rastrear las direcciones web y asegurar que no quede traza de las claves utilizadas.
- Asimismo, debe evitar el uso de servicios públicos o gratuitos de wi-fi (como los que se encuentran comúnmente en las bibliotecas públicas y cafeterías). En caso de que sea necesario hacer uso de éstos, deberá asegurarse de que se cumplan los requisitos de seguridad descritos en la Políticas de Seguridad de Redes. Una vez que se finalice la navegación, deberá cerrar las sesiones y borrar cualquier traza de información que quede en el equipo.
- El trabajador remoto debe evitar transmitir la información clasificada de **uPlanner**, (incluido el envío de su nombre de usuario y contraseña) a través de una red insegura (por ejemplo, una página web que no comience con "https") o en los casos de que no disponga de VPN.

En relación a los equipos

Los colaboradores se aseguran de que todo equipamiento tecnológico (incluidos los teléfonos inteligentes o smartphones) utilizado para trabajar con información de **uPlanner** de forma remota o en movimiento, se haya protegido de acuerdo a lineamientos entregados por la **Gerencia Responsable** y por **el Senior Cloud Systems Administrator.**

Los dispositivos personales que contengan información de **uPlanner** deberán contar con protección de acceso (vía huella, patrón o similares). Asimismo, se habilitará rastreo remoto y borrado remoto para los casos de hurto o extravío.

Todo empleado de **uPlanner** debe informar al **Senior Cloud Systems Administrator** de la pérdida de su equipo conteniendo información de la empresa. Previo al envío a servicio técnico, se deberá eliminar toda información de la organización; se preferirá la renovación del equipo dentro de lo posible.

Acceso remoto

Se pide al trabajador remoto que utilicen métodos de acceso seguro con VPN para acceder a la información clasificada y aplicaciones de **uPlanner**, y que la información, en lo posible, no debe ser descargada en el dispositivo remoto o móvil. Dado que esto último escapa a los conocimientos habituales de los usuarios de teléfonos móviles, el **Senior Cloud Systems Administrator** podrá emitir instructivos de limpieza periódica de datos.

Adicionalmente, el trabajador remoto deberá resguardar las claves de accesos de todos los dispositivos en medios de resguardos dispuestos por **uPlanner**. Estas no deben ser guardadas de ningún modo en un archivo local del equipo ni tampoco compartida con terceros.

Transferencia, sincronización y uso compartido de archivos

El trabajador remoto debe asegurarse de que el uso de cualquier herramienta de transferencia de archivos (incluido el correo electrónico), la sincronización y el uso compartido para el trabajo remoto o móvil, cumpla con los procedimientos de clasificación y manejo de la información. Las herramientas aprobadas por **uPlanner** para compartir información se definirán e informarán a los empleados y colaboradores.

El trabajador remoto no debe configurar la sincronización de carpetas "en la nube" en computadoras portátiles o estaciones de trabajo que no estén autorizadas y configuradas según los lineamientos de **uPlanner**.

Responsabilidades especiales

Las jefaturas son responsables de asegurar que el personal tome conocimiento de la presente política para el trabajo remoto.

Cuando los requisitos de la política dependen de cada trabajador de manera individual, serán personalmente responsables de aplicar las políticas, procedimientos o procesos definidos. Los trabajadores asimismo tendrán la obligación de informar respecto de cualquier deficiencia en los controles de seguridad o cuando haya ocurrido un incidente.

6.12 Gestión y Protección del uso de los dispositivos

La Gestión y protección del uso de los dispositivos tiene como objetivo establecer los lineamientos para una adecuada utilización de los activos de información de la compañía por parte de los usuarios incluyendo colaboradores, proveedores y terceros contratados.

Por lo que se toman las siguientes medidas recomendadas:

- Eliminar aplicaciones que no se usen o necesiten en los computadores.
- Actualizar el sistema operativo y aplicaciones de forma regular.

- Mantener el firewall del computador encendido, en base a las necesidades del trabajo del profesional.
- Para los usuarios de **Windows**, asegurar la instalación de un software antimalware o utilizar Windows Defender, y mantenerlo actualizado. Para usuarios **Mac**, considerar usar un antimalware.
- Guardar documentos en espacios de almacenamiento oficiales de la empresa para que estén respaldados de forma apropiada y disponibles ante cualquier emergencia.
- Mantener encendido el cifrado de disco.
- Tener cuentas separadas para otros usuarios como familiares, en el caso de que utilicen el computador que se utiliza para actividades de la compañía. Idealmente, tener computadores separados para el trabajo y para uso de la familia u otros.
- No usar un administrador de cuentas en el computador de uso diario.
- No compartir bajo ningún concepto las credenciales de acceso a los diferentes sistemas, plataformas y aplicativos como así tampoco escribir las contraseñas en lugares donde otras personas puedan visualizarlas.
- No abandonar el puesto de trabajo sin antes desconectarse del sistema o de activar el salvapantallas con contraseña, de forma tal de impedir la utilización de los perfiles, por personal no autorizado.
- Proceder a cambiar la contraseña en forma inmediata cuando sospeche que se encuentra comprometida.

6.13 Gestión de Claves y Criptografía (Control A.10.1.1)

La gestión de la criptografía tiene como objetivo proporcionar un nivel más alto de seguridad de la información para que ésta no pueda ser leída por personas no autorizadas.

Y para esto, uPlanner utiliza métodos criptográficos que protegen la confidencialidad e integridad de su información, no solo durante su almacenamiento, sino también durante su transferencia y recepción.

Estos métodos son aplicados en los siguientes elementos:

- Credenciales de accesos.
- Información compartida por medios no oficiales (archivos, correos electrónicos, etcétera).
- Información y repositorios de backups.
- Información interna restringida para la mayoría de los empleados.
- Bases de datos.
- Registros de usuarios.
- Información de carácter personal.

Además, para ejecutar un protocolo de seguridad de criptografía eficiente, uPlanner considera lo siguiente:

- El establecimiento y gestión de las claves públicas y privadas, lo cual se realiza siguiendo el Procedimiento de Gestión de Claves Públicas y Privadas definido por la empresa.
- La autenticación de los usuarios.
- La aplicación de cifrado de mensajes y métodos de no repudio.

La organización establece que los métodos criptográficos a implementar son:

Activo de información	Método criptográfico	Especificaciones
Firma de documentos digitales	Firma electrónica	DocuSign
Almacenamiento de información en la nube	Cifrado simétrico	AES
Accesos a plataformas en trabajo remoto.	VPN	OpenVPN

Mensajería por correo electrónico confidencial	Cifrado asimétrico	Estándar Open PGP

Para garantizar una adecuada gestión de las claves (incluida su criptografía) de acuerdo con las mejores prácticas de seguridad de la industria y a los requerimientos normativos que aplican a la compañía.

Por tal, se dictamina:

- Los integrantes del equipo no deben compartir contraseñas, si un miembro del equipo requiere un usuario y/o contraseña para acceder a un servicio, el mismo debe solicitarlo al Jefe de Área, el cual se encargará de darle los accesos solicitados.
- Las contraseñas generadas por equipo deben poseer como mínimo una longitud de 8 caracteres y contener minúsculas, mayúsculas, números y símbolos. Un ejemplo de esto puede verse en el siguiente texto: "7_#{P>_[4M(5UpA\FpRuy>+5"
- Los integrantes del equipo deben utilizar un gestor de contraseñas, los recomendados por el equipo son: KeePass.
- Todas las aplicaciones utilizadas por el equipo deben ser configuradas con segundo factor de autenticación (2FA) y los códigos de backup deben ser almacenados de forma segura en un gestor de contraseñas.
- Debe evitarse compartir credenciales en texto plano por medios no seguros.
- No escribir PINs y contraseñas al lado de computadores o teléfonos.
- Cambiar las contraseñas de manera regular y cuando se sospeche compromiso.
- No utilizar la misma contraseña para diferentes sistemas críticos.
- Considerar el uso de criptografía sólida en todos los aplicativos que estén sometidos a normativas que regulan el negocio.

6.14 Gestión de Respaldo, Recuperación y Continuidad

La Gestión de Respaldo, Recuperación y Continuidad tiene como objetivo establecer lineamientos tendientes a la preservación de los datos, operatoria y poder asegurar la continuidad del negocio.

Para esto, es necesario:

- Asegurar un inventario de los soportes de resguardo existentes, su contenido y lugar de almacenamiento, así como también fijar los responsables de mantener esos inventarios y mantener una copia actualizada del mismo en una locación remota.
- Realizar pruebas periódicas de recuperación de información desde los soportes almacenados con el fin de asegurarse del adecuado funcionamiento de los procesos de generación de las copias y de la disponibilidad de la información en tiempo y forma.
- Realizar un análisis de riesgo para determinar cuáles son las amenazas y escenarios de desastre a las que se encuentran expuestos los procesos críticos, cuál es su probabilidad de ocurrencia y cuál es su impacto económico en caso de que ocurra una contingencia.
- Establecer los medios para que todo el personal clave involucrado en el DRP pueda ser contactado y ubicado en forma inmediata, como así también establecer los procedimientos de Comunicación de Crisis necesarios durante la contingencia y hasta que sea normalizada la operación.
- Definir, documentar, ejecutar y controlar un plan de pruebas anual para la evaluación de la eficiencia del plan de continuidad del negocio y la detección de mejoras a implementar y necesidades de capacitación.
- Elaborar, revisar, actualizar y documentar el BIA como fuente de información y respaldo a las decisiones del negocio relacionadas con nuestro alcance del plan de continuidad del negocio.

También, se consideran las respuestas a las potenciales interrupciones al negocio:

- Interrupción severa del transporte.

- Incapacidad de acceder a la oficina por inundaciones, fuego, desorden civil, incidentes terroristas, etcétera.
- Pérdida de internet y/o conexión telefónica.
- Pérdida o robo de sistemas críticos.

Los planes de contingencia se probarán, al menos, una vez al año.

6.15 Gestión de Relaciones con Proveedores

Establecer lineamientos para la administración de proveedores de servicio, de manera tal de reducir los riesgos inherentes a trabajar con terceros y así contribuir con la protección de la información confidencial de la organización y la de sus clientes. Para esto, es necesario:

- Mantener una lista de los proveedores de servicios, que incluya entre otros, su clasificación y la descripción detallada del servicio prestado.

- Existir un procedimiento formal para contratar a proveedores de servicio que incluya la debida diligencia antes de la contratación.

- Contar con un contrato por escrito con cada proveedor relacionado con el alcance en materia de Protección de Datos. El mismo debe incluir la responsabilidad que el proveedor posee sobre la seguridad de los datos (almacena, procesa o transmite en representación de **uPlanner** o que podría afectar la seguridad de los datos de los clientes).

- Definir los requerimientos mínimos de seguridad para cada tipo de información y el tipo de acceso que servirá como base para los acuerdos individuales por proveedor con base en las necesidades de negocio, requerimientos y el perfil de riesgos de la organización.

- Definir los tipos de obligaciones aplicables a los proveedores para proteger la información de la organización.

- Contar con procedimientos para el manejo de incidentes y contingencias asociadas con acceso del proveedor incluyendo responsabilidades tanto de la organización como de los proveedores.

- Si el proveedor proporciona información confidencial a **uPlanner**, se debe asegurar que se cumplan los acuerdos de confidencialidad.

- Contar con una gestión adecuada de los cambios que puedan presentarse en los contratos de los proveedores. Contemplar tanto cambios que se deriven de la relación directa con el proveedor, así como de cambios realizados en uPlanner que afecten directa o indirectamente a estos.

6.16 Gestión de Cumplimiento

La Gestión de Cumplimiento tiene como objetivo establecer lineamientos tendientes a estar alineados con las diferentes regulaciones y normativas a las que la empresa esté sujeta.

Para esto, es necesario:

- Verificar que los acuerdos con clientes internos (empleados), clientes externos (clientes) y proveedores, cumplan con las pautas de las regulaciones e incluyan aspectos relacionados a los riesgos de seguridad de información derivados del servicio prestado.
- Determinar puntos de control con los terceros subcontratados en cuanto al cumplimiento de las mejores prácticas y normativas.

- Establecer las políticas y procedimientos necesarios para establecer el marco de adherencia y control a las regulaciones.
- Llevar a cabo las revisiones de cumplimiento de seguridad de la información, se recomienda que de manera **anual** se realice el plan de auditoría por personal externo.
- De manera periódica, realizar el plan de verificación de los sistemas de información, por medio de una evaluación donde se verifique que los mismos se encuentran configurados de acuerdo con las reglas y políticas definidas.

7 Versionado

Confeccionado por:	José Garagorry (SCSA)
Código de documento:	DOC-ISO-05
Versión:	V3
Fecha última de actualización:	25/10/2023
Revisado por:	• Mayra Abarca (CSA) • Daniela Hellman (BI Engineer)
Aprobado por:	Comité de Seguridad de la Información.
Comunicado a:	Todos los colaboradores de uPlanner.
Fecha aprobación	25 / 10 / 2023
Clasificación de esta información:	• Información Pública.